| Policy | |
|---|---|

# IT SECURITY POLICY

| | |
|---|---|
| **Department / Service:** | All |
| **Originator:** | Countywide IT Services Gloucestershire |
| **Accountable Director:** | Chief Executive Officer |
| **Approved by:** | IG & Records Management Committee |
| **Date of approval:** | June 2021 |
| **Revision Due:** | June 2023 |
| **Target Organisation(s)** | Tetbury Hospital Trust Ltd |
| **Target Departments** | All |
| **Target staff categories** | All |

**Policy Overview:**

This document defines the recommended IT Security Policy for stakeholders in the Gloucestershire Countywide IT Shared Service. It should be adopted as a corporate, non-clinical policy by each trust which participates in the shared service. The IT Security Policy applies to all business functions and information contained in electronic format within the Trust, the physical environment and people who administer, support and use the IT Service. This policy will not be adapted to Tetbury Hospital IT structure.

**Key amendments to this Document:**

| Date | Amendment | By: |
|---|---|---|
| 3/15 | Adopted from Countywide IT Services | JJ |
| 11/18 | First revision/update to GDPR | JJ |
| 6/21 | Updated by CITS – Policy readopted – Rob Holmes | JJ |
| | | |
| | | |
| | | |
| | | |

| Policy | | TETBURY HOSPITAL |
|---|---|---|

TRUST POLICY

# IT SECURITY

**This document may be made available to the public and persons outside of the Trust as part of the Trust's compliance with the Freedom of Information Act 2000.**

**Please be aware that only documents downloaded or viewed directly from the GHNHST Trust Policies webpage are valid documents. Documents obtained through printed copies or internet searches may be out of date and therefore will be invalid.**

**FOR USE BY:**
**This Policy is to be followed by all staff of Gloucestershire Hospitals NHS Trust and Gloucestershire Managed Services – Staff will need to be on the secure HSCN network to be able to view these additional documents**

**FAST FIND:**

- **RD1 - IT Security Policy Document Matrix and Quick Guide**
- **AC1 – IT Access Control**
- **AC2 – Registration and de-registration**
- **AC3 – Password usage and management**
- **AC4 – Physical and environmental security**
- **AC5 – Purchase and disposal of equipment**
- **AC6 – Fax protocol**

## 1. INTRODUCTION

This document is the IT Security Policy for Gloucestershire Hospitals NHS Foundation Trust and defines the recommended IT Security Policy for other stakeholders in the Gloucestershire Countywide IT Shared Service. It should be adopted as a corporate, non-clinical policy by each Trust which participates in the shared service.

This policy applies to all business functions and information contained in electronic format within the Trust, the physical environment and people who administer, support and use the IT Service.

This policy is supported by a framework of other documents covering aspects of the development, operation and use of the Trust's IT infrastructure – see the IT Security Policy Document Matrix and Quick Guide.

Read this document in conjunction with the Information Governance policy. The legal framework for this policy includes:

- The General Data Protection Regulation 2016
- Data Protection Act 2018
- Computer Misuse Act (1990)
- Copyright Designs & Patents Act (1988)

- Regulation of Investigatory Powers Act (2000)

The Trust may grant exception to this policy if there is a genuine business requirement, but this may only be granted after an assessment, in accordance with the Risk Management Strategy and with approval of an appropriate executive director in agreement with the director responsible for IT Services.
This policy applies to all individuals who access or process data held by the Trust, whether directly employed by the Trust or contractors, third party service providers and private sector care providers.

Wilful or negligent disregard of this policy will be investigated and dealt with under the Trust Disciplinary Procedure.

## 2. DEFINITIONS

| Word/Term | Descriptor |
|---|---|
| **Senior Information Risk Owner (SIRO)** | An executive who is familiar with and takes ownership of the organisation's information risk policy and acts as advocate for information risk on the Board |
| **Chief Information Officer (CIO)** | Senior manager responsible for managing and escalating information risk |
| **Information Assets (IAs)** | Identifiable and definable assets owned or contracted by an organisation, which are valuable to the business of the organisation. These include:<br>▪ Information – databases, system documents and procedures, archive media/data<br>▪ Software – application programs, systems, development tools and utilities ▪ Physical – infrastructure, equipment, furniture and accommodation used for data processing<br>▪ Services – computing and communications, heating, lighting, power, air conditioning used for data processing<br>▪ People – their qualifications, skills and experience in use of information systems<br>▪ Less tangible elements – these can include the reputation and image of the organisation |
| **Information Asset Owner (IAO)** | Senior individuals involved in running the relevant business. Their role includes understanding, documenting and addressing security risks affecting the information assets they own, and to provide assurance to the SIRO on the security and use of those assets |
| **Information Governance Forensic Readiness** | The ability of an organisation to make use of digital evidence when required. Its aim is to maximize the organisation's ability to gather and use digital evidence within the law whilst minimizing the disruption or cost in doing so |
| **IT Security Incident** | Any breach or potential breach of information/security, physical or computer related |

## 3. PURPOSE

The main objective of this policy is to ensure that electronic data is protected in all of its forms, during all phases of its life cycle, from unauthorized or inappropriate access, use, modification, disclosure or destruction, through the application of the standards and definitions of the ISO27000 series of standards as used in the NHS Data Protection and Security Toolkit.

This policy applies the key concepts of Information Assurance to electronic data processing in the Trust; namely,

- Confidentiality

- Integrity
- Availability
- Accountability

## 4. ROLES AND RESPONSIBILITIES

| Post/Group | Details |
|---|---|
| **All Staff** | • Accountable for the function they perform using IT equipment<br>• Undertake mandatory training in Information Governance and Information Security<br>• Abide by the principle of the GDPR and the Data Protection Act and other relevant legislation and information<br>• Ensure familiarity with Trust IT security measures and that these are properly maintained<br>• Promote a culture that values the Confidentiality, Integrity and Availability of Trust IT information assets |
| **Department Managers** | • Ensure that departmental IT processes are up to date and regularly reviewed<br>• Ensure that departmental risk registers are regularly reviewed and acted upon<br>• Communicate changes to IT security policy/best practice to department Line Managers<br>• Ensure that departmental mandatory training is completed to required standards |
| **Line Managers** | • Ensure that staff are provided with the correct IT equipment and training to perform their roles in a safe and secure manner<br>• Regularly review staff compliance with training, certification, applicable legislation<br>• Communicate changes in policy/best practice to staff<br>• Log and report security incidents, escalate as appropriate<br>• Encourage staff to adopt an open approach to reporting information security incidents |
| **Information Asset Owners (IAOs)** | • Understand what information is held on their assets<br>• Understand how information is added to, moved within and removed from their assets<br>• Understand who/which systems have access to the information asset and ensure that use is monitored<br>• Understand and assess the risks to Confidentiality, Availability and Integrity to information held on their assets and escalate in line with Trust Risk Management policy<br>• Ensure that information assets are recorded in the Organisation's information asset register<br>• Provide written input to the Senior Information Risk Owner on the security and use of assets under their control (annually)<br>• Ensuring information is used within the law |
| **Information Asset Administrators (IAAs) or System Administrators** | • Control access to the asset for which they are responsible<br>• Ensure the delivery of appropriate training to users of the asset<br>• Ensure processes are properly documented and available for dissemination to all relevant users<br>• Record and act upon security incidents<br>• Ensure the integrity of information held or processed<br>• Agree change control processes relating to the system |

| | |
|---|---|
| **IT Service Providers** | • Responsible for the compliance of their services with this policy<br>• Demonstrate robust processes for the identification & mitigation of IT risk<br>• Understand the information risks and support each Organisation's response<br>• Ensure that the Organisation is kept up to date and briefed on all information risk issues<br>• Support the Organisation's approach to IT risk through effective resource, commitment and execution of the SLA<br>• Ensure that identified IT threats and vulnerabilities are followed up for risk mitigation in accordance with the Organisation's requirements<br>• Provide support for Information Asset Owners (IAOs) of the Organisation through effective IT support |
| **Chief Information Officer (CIO) and Senior Information Risk Owner (SIRO)** | • Understand the information risks and lead the Organisation's response Ensure that the Board and the Accountable Officer are kept up to date and briefed on all information risk issues affecting the organisation and its business partners<br>• Ensure that the Organisation's approach to IT risk is effective in terms of resource, commitment and execution<br>• Own the assessment processes for information risk<br>• Ensure that there are effective mechanisms in place for reporting and managing Serious Untoward Incidents (SUIs) relating to the information of the Organisation<br>• Ensure that identified IT threats and vulnerabilities are followed up for risk mitigation, and that perceived or actual IT incidents are managed in accordance with NHS IG requirements<br>• Provide input into the management of Serious Untoward Incidents (SUIs) relating to the information of the Organisation<br>• Provide leadership for Information Asset Owners (IAOs) of the Organisation through effective networking structures, sharing of relevant experience/industry best practice, provision of training and creation of information risk reporting structures |
| **Information Governance Manager** | ▪ Responsible for information assurance within the Trust as such aspects as interrelate with this policy<br>▪ Accountable for the compliance of the Trust's IT services with this policy, and for the development of subsidiary policies and procedures relating to the use and management of the Trust's IT infrastructure<br>▪ Maintenance and review of this policy in line with legislation and national guidelines |
| **IT Security Officer** | • Responsible for identifying device configurations and software requirements that the Trust may require in order to comply with this policy, and Information Governance and Security policies and standards |
| **Data Protection Officer** | required by Article 37 GDPR including:<br>• to inform and advise the Trust and its employees of their obligations pursuant to the Data Protection Legislation<br>• to monitor compliance with the Data Protection Legislation<br>• to provide advice as regards data protection impact assessments and monitor their performance |

## 5. THE NEED FOR IT SECURITY

With increased public awareness of identity theft and the power of information, information security is the area of the Trust's operations that most needs control. Without information the Trust could not function, so valuing and protecting the Trust's information are crucial tasks.

Security is everybody's business and therefore everyone has a responsibility to ensure information is appropriate, secure, confidential, accurate and available only to authorized users. Without effective security, Trust Information Assets may become unreliable and untrustworthy,

may not be accessible where or when needed or may be compromised by unauthorized third parties

This policy sets forth requirements for the incorporation of information security practices into the daily usage of Trust systems, to help ensure that the Trust is not exposed to legal and governance risks from the use of electronic communications and the internet, and that its reputation is not adversely affected.

Violation of this policy may result in damage to the Trust's reputation, significant financial penalties, and disciplinary action up to and including dismissal.

## 6. IT SECURITY MANAGEMENT STRATEGIES

### 6.1 Risk assessment

It is the responsibility of the IAOs of each Organisation to carry out local risk assessments.

The risk assessment will identify the appropriate countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

The information gained from risk assessments will be used to develop risk management strategies and processes to ensure that IT security risks are mitigated wherever possible (see 6.2 below).

Where risks cannot be mitigated, the organisational risk managers are responsible for ensuring that these are entered on to the Trust's risk register.

### 6.2 Trustwide management of IT security risks

The organisational IG managers are responsible for ensuring that all IT security risks are managed as far as is reasonably practicable.

The risk management strategies used includes:

- **Appointing named individuals** to undertake defined roles relating to IT security and information governance. See the individuals identified in section 'ROLES AND RESPONSIBILITIES' section, above.
- **Applying robust access controls** to protect the information processed and stored in Trust IT and physical systems. These measures are applied to protect the confidentiality and integrity of data held, and also to ensure compliance with legislation such as the GDPR and Data Protection Act
- Ensuring there are robust security requirements for **setting up user accounts, enabling user access and ensuring the user is properly authenticated** to access Trust IT systems. This measure will also mitigate the risk of unauthorized access of information; establish user accountability and rules for access. This will also include clear policy guidance on the registration and deregistration of staff requesting access to Trust IT facilities
- Defining a **password management policy** which stipulates the need for "strong passwords" and the management controls to ensure passwords are protected

- Ensuring that the use of all **mobile devices, removable media and "bring your own" devices** are appropriately controlled, including the use of encrypted devices where any Person Identifiable Data is used or stored on one of these devices
- Ensuring a robust **security incident management procedure** is enacted. Damage to the Trust from IT security incidents can be minimized by monitoring and acting upon them effectively
- Ensuring that Project Managers and others who implement systems include **effective security countermeasures as part of the specification and implementation as part of any new systems project**. This will include the completion of a privacy impact assessment. Identification of an information asset owner and registration as an asset on the Trust's information asset register
- Ensuring that all **information systems, applications and networks are approved by the director responsible for IT services before they commence operation**. Also to ensure that information systems do not pose an unacceptable security risk to the organisation. Clinical systems providers must record risk associated with their systems; IAOs will receive risks and ensure mitigation is in place
- Ensuring that the **purchase and disposal of IT equipment and media** is appropriately controlled to protect information assets
- Ensuring that there are appropriate **security measures** to protect Trust-owned IT equipment
- Ensuring the production and maintenance of **comprehensive policies and procedures** relating to all of the above, which are clear and disseminated to all relevant users. These are listed in the IT Security Policy Document Matrix and Quick Guide.
- Providing **mandatory training** to all staff in Information Governance and IT Security
- Maintaining an information asset register which identifies the data held within an asset, the lawful basis for holding any personal data, access and other security controls, associated information flows, and processing records required by GDPR Article 30
- Ensuring that where appropriate there is a system level security policy for an asset. This shall be mandatory for any asset identified as business critical
- Meeting the requirements of CareCERT and protecting web applications against OWASP flagged vulnerabilities
- Meeting the National Data Guardian's Security standards

### 6.3 Local management of IT security risks

Information Asset Owners, Information Asset Administrators and Systems Managers are responsible for ensuring the following:

- That there are clear and robust local procedures relating to the operation of the systems under their control, to include user access controls and access rights
- That local procedures are developed in response to risk assessments
- That assets are recorded in the information asset register and reviewed at least annually

### 6.4 Forensic readiness

The Trust has approved the introduction of Information Governance (IG) forensic readiness into its business processes and functions; in order to maximize the potential to use digital evidence whilst minimizing the cost of investigation by actively collecting potential evidence. This evidence may be collected in advance of a crime or incident and will be used to the benefit of the organisation, its patients and staff. For example, the Trust may employ logging software to

determine detailed user and machine interactions with files stored on the network, which might include details of when files are accessed and by whom, when/if they are transferred off the network and/or shared with other users, when they are moved to another network storage location and when/if they are deleted. This decision reflects the high level of importance placed upon minimizing the impacts of information security events.

## 7. TRAINING

All users are required to have an awareness of this policy and its related documents.

## 8. MONITORING OF COMPLIANCE

| | |
|---|---|
| Do the systems or processes in this document have to be monitored in line with national, regional or Trust requirements? | YES |

| **Monitoring requirements and methodology** | **Frequency** | **Further actions** |
|---|---|---|
| Compliance with policy by all staff via audit and DSP Toolkit return, coordinated by Trust IG/IT leads | Annual | Recommendations from IT Security Panel will be presented to IM&T Board |
| Exception monitoring of Datix Web reports by Trust IG/IT leads | Bi-monthly | Monitored by IG Core Group, issues reported to the IG and HR Specialist Group |
| Monitoring of breaches reported to the IT Service Desk by service desk leads | Ongoing | Reviewed by IT Security Officer, escalated to IG/IT leads. Further escalation via IT Security Panel. |

**IT SECURITY (POLICY)**

| **DOCUMENT PROFILE** | |
|---|---|
| REFERENCE NUMBER | B0591 |
| CATEGORY | Non-Clinical |
| VERSION | V4 |
| DIVISION | Owning Division – Corporate |
| SPECIALTY | Owning Specialty - Information Governance<br>Associated Specialities - Cyber Security (IT Services) |
| FOR USE BY | GHNHST & GMS STAFF |
| QUALITY ASSURANCE GROUP | Information Governance & Health Records Committee (IGHR) |
| AUTHOR | Rob Holmes, IT Security Officer<br>Phil Bradshaw, Information Governance Support Officer |
| ISSUE DATE | February 2020 |
| REVIEW DATE | February 2023 |
| OTHER APPROVING GROUPS | Countywide Cyber Security Group |

| | |
|---|---|
| APPROVAL AND RATIFICATION DETAILS / DATES | Policy Approval: IG and HR Committee dated 26/03/2019 TPAG Approval: 02/10/2019 |
| EQUALITY IMPACT ASSESSMENT | B0591 EIA |
| CONSULTEES | Countywide IT Security Panel; IT Operational Group |
| DISSEMINATION DETAILS | Upload to Policy Site; global email; copy of policy will be issued to all staff authorised to use IT systems within the Trust. Updated guidance and specific security alerts will be issued by global or targeted communications from IT Services or Information Governance on an ad hoc basis |
| KEYWORDS | Security, IT, risk assessment |
| RELATED TRUST DOCUMENTS | RD1 - IT Security Policy Document Matrix and Quick Guide<br>AC1 – IT Access Control<br>AC2 – Registration and de-registration<br>AC3 – Password usage and management<br>AC4 – Physical and environmental security<br>AC5 – Purchase and disposal of equipment<br>AC6 – Fax protocol |
| OTHER RELEVANT DOCUMENTS | Trust Disciplinary Procedure<br>Information Governance Policy |
| EXTERNAL COMPLIANCE STANDARDS AND/OR LEGISLATION | The Data Protection Act (2018)<br>General Data Protection Regulation 2016<br>Computer Misuse Act (1990)<br>Copyright Designs & Patents Act (1988)<br>Regulation of Investigatory Powers Act (2000) |

| ACTION CARD | |
|---|---|
| **TITLE: Purchase and Disposal of Equipment** | **B0591 AC5** |
| **FOR USE BY:** Asset Owners | **LIAISES WITH:** Procurement, IT Service Desk |

**Applicable equipment:**
IT equipment covered by this process includes:

- Personal computers (PC) and Laptop computers
- Servers
- Printers/Fax/Scanner
- Data disks including Encrypted USB memory sticks
- VDU Screens
- Cables
- Print waste Zebra film roles

**Purchase:**

- All IT equipment purchase is managed by Procurement, who will advise on current Trust supplier contracts
- The IT department can give advice on specific equipment requirements prior to contacting Procurement

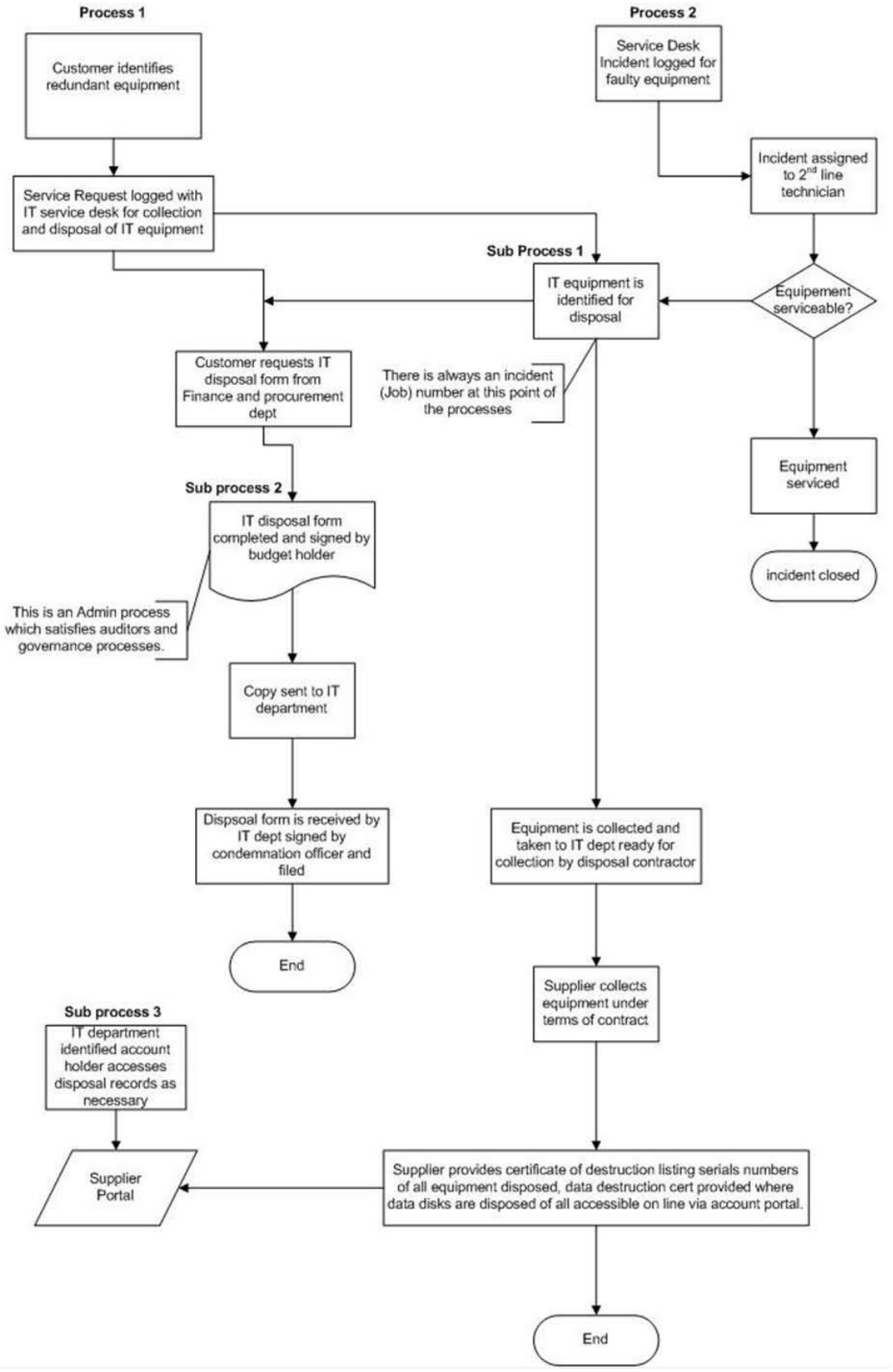
**Disposal:**

- The process is managed day to day by Countywide IT Services – IT equipment is classified as hazardous waste due to the make-up of the electronic components
- All disposals must be carried out according to the flowchart on page 2
- Collections will only be carried out as part of an incident or service request – there must be a job/work reference
- All items disposed of must be recorded and/or logged for future reporting and audit. This may be supplier provided, local systems records, or a combination of the two
- All items for disposal must be authorised by the budget holder
- 2gether Mental Health Trust users are required to complete an **IT Equipment Disposal Request**

**Ensuring data security when disposing of equipment:**

- Media which require secure disposal includes CD/DVD, hard disk drives, memory sticks, magnetic tapes/cartridges used for backups and voice/video tapes used in surveillance systems
- Equipment must not be thrown into a skip or sold on to Trust staff at the end of the equipment's use
- All data on IT equipment must be destroyed before it leaves the premises, or by the third party contractor
- All software must be removed unless there is documented agreements between the software supplier and the disposing organisation that the licence will be transferred

**Generic Process Flow**



| ACTION CARD | |
|---|---|
| **TITLE: Physical Access to IT Equipment and Systems** | **B0591 AC4** |
| **FOR USE BY:** IT Support Staff, Estates | **LIAISES WITH:** System/Service Suppliers |

Information processing resources including buildings, offices, computer equipment, electronic services, communication media and paper based records must be protected from unauthorised access, misuse, damage or theft.

**Building/environmental security:**

- All IT service facilities that support critical and/or sensitive business activities must be housed in secure areas which are protected from unauthorised access, damage and interference • Rooms must be lockable and windows secure to break-ins
- Consider the use of alarm systems and mechanisms to make equipment physically secure and difficult to remove
- Site IT equipment in areas with air conditioning if possible
- Ensure IT equipment rooms are fitted with fire suppressant systems or provided with fire extinguishers

**IT equipment power supply:**

- Critical IT equipment must be protected from power outages, brownouts, power spikes and other electrical anomalies
- Power and telecommunications lines into IT facilities must be protected against electrical anomalies

**Entry controls:**

- Door codes must be given to authorised personnel only
- Change door codes annually
- Ensure all staff accessing secure areas carry a valid ID
- Supervise visitors and record times of their arrival and departure

**IT Equipment in public areas:**

- Ensure screens and printers are positioned so that confidential information cannot be seen by unauthorised persons

**IT equipment maintenance:**

- All IT maintenance must be carried out by IT department staff or an approved contractor
- Where an approved contractor is used, written contracts must be maintained which include confidentiality clauses. Risk assessments must be carried out prior to contracts being awarded.

**Security of systems and data off Trust premises:**

- Equipment, data, software or paper records must not be taken off site without documented management authorisation
- All portable devices, media-holding software or data (including paper records) must be protected against damage or theft and not left unattended in any circumstances

ACTION CARD
TITLE: Password Usage and Management B0591 AC3
FOR USE BY: All employees, volunteers, contractors and consultants; any other individuals who have been given access to the Gloucestershire Healthcare Community network, including guests LIAISES WITH: IT Service Desk, Information Asset Administrators

**Protecting passwords:**

- Individuals are **personally responsible** for protecting their passwords. Any PC left unattended and logged in can give access to an unauthorised user
- Users are responsible for all use of information systems, and any information stored or communicated using their identity or password
- All user names are unique and are not reused – treat your user name as personal
- Passwords may only be shared in **exceptional** circumstances when an IT specialist is present; change the password as soon as the IT specialist has finished work on the system
- **DO NOT** share passwords over the phone or by email.

**Password storage and configuration of Microsoft Windows systems:**

- System administrators must ensure that where passwords are stored in systems, they are hashed/encoded
- Where possible, configure Microsoft Windows systems to not store LM hash value of user's passwords

**Password complexity and choice:**

- **Password Complexity** - users are required to choose strong passwords.
- **Password Choice** - passwords must be chosen to protect the user's 'electronic identity', prevent unauthorised access to systems and preserve the availability and integrity of data – see guidance on page 3. Do not recycle passwords.

**Password aging and forced password change:**

- **Forced Password Change** - Administrators/System Managers who operate systems independent of Active Directory must ensure that newly created accounts for a password change at first log-on, where this is technically possible.
- **Password Aging** – Network access passwords must be changed at least every 90 days – the system will prompt users to do this.

**Unforced password changes:**

The following are required:

- **Users at Initial Logon** - Users of systems that cannot be configured to force-change their initial default passwords at first logon are required to change them themselves at the first logon.
- **Default Passwords** - System administrators and IT support staff who configure new systems and set up services must ensure that all password settings are changed from default before moving platforms into production.
- **System Level Passwords** – change at least quarterly, or preferably monthly.

- **User Passwords** – Change at least every 90 days, or if a password has been compromised.
- **Temporary Account Passwords** – change every time a temporary user leaves or no longer needs access to the account.

Apply a new and unique password every time a temporary account is used/issued (does not apply to training accounts)

**Systems-level (administrator and super-user) passwords:**

- These are only issued on a "need to know" basis.
- Do not use shared administrator and super-user (global) passwords on production systems except where hard-coded into applications. Consider applying this rule to development and research systems.
- On Windows systems, passwords for privileged accounts must be **15 characters or more**, and follow the password choice rules below. (cont)
- Administrators and IT support staff are to be allocated secondary accounts which have the appropriate rights and privileges to enable them to support the systems and services for which they have a responsibility. This should be done in all cases where hard-coded passwords are not required

TITLE: Password Usage and Management B0591 AC3
FOR USE BY: All employees, volunteers, contractors and consultants; any other individuals who have been given access to the Gloucestershire Healthcare Community network, including guests LIAISES WITH: IT Service Desk, Information Asset Administrators

**Hard-Coded and Service Account Passwords:**

- Hard coded and service account passwords must never be used to log onto servers.
- Change passwords on a quarterly basis, and synchronise to avoid operational problems. Where password changes are due on a Friday they are to be deferred until the next working day
- These passwords are to be held securely for Disaster Recovery purposes in a series of sealed envelopes along with a log of when they were accessed. Normally when a sealed password has been accessed it must be changed after use.

**Shared Passwords:**

- Passwords are not to be shared by users, except in the case of administrators and IT Support staff that are responsible for the maintenance of systems and services that utilize hard-coded passwords.
- Where there is a need for several users to have access to common data and mail boxes, such as those working collaboratively, contact the IT service desk for guidance

**Compliance Monitoring:**

Password cracking tools may be operated by the IT Service on a random or periodic basis in a bid to identify weak passwords. Authority must first be obtained from the IT Service Security Coordinator.

**Password Resets:**

- The identity and association of a person with a particular account must be verified by administrators prior to resetting their password.

- Passwords must not be re-set on the basis of an e-mail request from the user regardless of the level of authority that the requestor may have.

Passwords must only be reset when the person requesting the reset is present and has been properly identified and verified against held documentation as being the account holder.

| ACTION CARD | |
|---|---|
| **TITLE: Registration and De-Registration** | **B0591 AC2** |
| **FOR USE BY:** All staff requesting access to Trust IT facilities (network, internet and email) | **LIAISES WITH:** Information Asset Owners, Information Asset Administrators, IT Service Desk |

**Rationale:**
This action card covers the following:

- Registration of all staff needing access to Trust IT facilities
- Removal/closing of accounts for leavers
- Retention of data directly associated with network accounts after individuals have left the Trust, i.e. emails and files that are only accessible by the individual user held on central servers

It does not cover the removal of access to individual applications or data in shared file areas or on individual PCs.

**Services provided:**
All Network activity is monitored by Trust approved software. The services available to authorised staff will include:

- **Internet Access** – site access is controlled by an Internet Filtering application.
- **Email Access** – the contents of which are monitored and filtered by a message manager application.
- **Network Access** – this will be defined by the member of staff role or work group

**Registration process – new accounts:**

- A New Accounts request form must be completed and signed by the staff member and their line manager. By signing the form, the user agrees to follow the Trust's requirements on IT security.
- The line manager must ensure that the form is accurately completed and submitted in good time – processing can take up to 1 week dependent on demand
- The IT Services department process the application form and set up the new account

**Registration process - name changes:**

- For name changes for any reason, the member of staff must contact the IT service desk
- The IT service desk will check the employee's security information before modifying any user details
- The IT Service Desk will ensure that emails to the previous name are redirected to the new name. The user will still be required to notify email contacts that their name has changed.

**Internal transfers between departments:**
IT services will not process these individuals as leavers unless requested.

- The outgoing manager must request the termination of specific access rights relating to their previous role which may no longer be appropriate.
- The new manager must request access rights pertinent to their new role.

An individual may be processed as a leaver if there is an issue about conflict of interest. The outgoing manager must inform the new manager of this action.

**Deregistration process – leavers (straightforward):**
When a user resigns from the Trust, the line manager must ensure the following:

- That the employee deletes non-business related emails and personal files are deleted
- That retained data and emails are moved so that future access of this information is possible
- That all key contacts of the leaver are notified of the replacement contact point

The leaver's account will be deleted as soon as possible after the user's termination date. Any emails sent to the leaver's email address will be modified so that the sender will receive an "undeliverable" message.

**Deregistration process – leavers (data clean up incomplete):**
If it has not been possible to achieve the clean up before the leaving date then the line manager can request that:

- The leaver's mailbox is made available to a nominated member of staff
- The leaver's new mail is diverted to the nominated member of staff's mailbox for a maximum period of three months.
- The leaver's data stored on personal file areas will be copied to a folder under the nominated user's personal file area.

The leaver's account will be deleted when these actions have been completed and after six months, or sooner if requested. Any emails sent to the leaver's email address associated with that account will be modified so that the sender will receive an 'undeliverable' message. The line manager must also Inform IT if any data stored in the closed account or in the archives will need to be retained for longer than 6 years.

| ACTION CARD | |
|---|---|
| **TITLE: Registration and De-Registration** | **B0591 AC2** |
| **FOR USE BY:** All staff requesting access to Trust IT facilities (network, internet and email) | **LIAISES WITH:** Information Asset Owners, Information Asset Administrators, IT Service Desk |

**Leavers who are not notified by line management:**
To manage this situation IT will process data from two different sources to ensure the network remains secure. In cases where IT cannot identify the staff member's line manager, IT will seek information from:

- **The ESR leavers list**; the information for the preceding month will be produced once payroll has closed. This information must be checked manually; where a leaver has no network account, no further action is required
- **Network logs**; A list of non-active accounts will be produced by accessing last log-on date information

**Leavers not notified by line management – deleting accounts process:**
If there is a potential match between a listed leaver and a network account then the following actions will be taken:

- An email will be sent to the leaver giving three weeks' notice that they are about to be processed as a leaver. This will allow for an incorrectly associated user the opportunity to respond before IT take any actions

After three weeks have passed:

- The network account will be disabled and the mailbox closed for incoming mail. If mail is sent to the mailbox an 'undeliverable' message will be received by the sender.
- The user will be removed from all distribution groups such as the global email groups Global CGH and Global GRH.
- The mailbox and personal data will remain in place to deal with any management requests for data access. These will be archived when the user appears on the disabled account report.

**Non-active account report:**
User accounts are listed with their last log on date. Accounts created more than three months ago and never used will be deleted. If the account has been unused for 12 months, IT Services will:

- Close the individual' network account and any associated mailbox. The mail box will be set up with an 'undeliverable' message for all incoming emails.
- The mailbox and personal data will be retained for audit purposes and to allow any management requests for data access to be met. These will be archived when the user appears on the disabled account report.
- The user will be removed from all distribution groups such as the global email groups

**Archiving of data:**
A monthly report will be run of accounts that have been disabled for three months or more. This will be processed in the following way:

- The personal data and email will be archived to offline storage.
- The individual's network account will be deleted.

Any request for data under the Freedom of Information Act 2000 will restore access to a nominated active user.

**Deletion of archived data:**
Annual reports will be run of data in the archive store. All archived data more than 6 years old will be permanently deleted. Managers are responsible for ensuring that all data held in e-mails is retained in accordance with the Trust agreed minimum retention period.

| ACTION CARD | |
|---|---|
| **TITLE: IT Access Control** | **B0591 AC1** |
| **FOR USE BY:** Users, Information Asset Owners, Information Asset Administrators | **LIAISES WITH:** IT Service Desk |

Access controls exist to protect the information processed and stored in IT systems. They are applied to protect the confidentiality and integrity of data held by the Trust and to help the trust comply with legislation such as the Data Protection Act. Access will be granted on the principle of **least privilege**. This means that members of staff will be provided access rights only to the level that they require in order to carry out their legitimate Trust business activities

**Controls:**

IT systems are subject to the following management controls:

| | |
|---|---|
| **Director of IT Services** | Responsible for overall IT security, defining the organisation's standards for access controls (usually a user name and password) and remote access |
| **Head of Information Governance** | Responsible for the Trust's register of Information Assets and records of third party and/or remote access |
| **Information Asset Owners** | Managing all risks associated with the systems under the control and implementing effective system level access controls |
| **Information Asset Administrators** | Manage day-to-day creation, modification and deletion of access control entries.<br>Ensure that new users are appropriately authorised, and adopt processes for reviewing and revoking access rights where required |
| **Line managers** | Request access levels for staff groups within their area, and maintaining appropriate records |
| **All staff** | Ensure their own system access details are kept secure and used in accordance with the Trust's business |

**General guidance:**

All access to systems must be authorised by its Information Asset Owner or nominated deputy.

Access to systems is not permitted when authorisation has expired (e.g. at the end of a project, or when an employee leaves the Trust). This applies even if accounts, access rules or access tokens have remained in place.

Any individual who discovers (intentionally or unintentionally) a means to bypass system access controls must report this promptly to their line manager or IT. Intentional abuse of access controls constitute a serious disciplinary offence and could also result in legal action.

Systems will be tested for resilience by competent persons under controlled conditions.

Users shall sign on with the least level of system privilege required for the particular task at hand.

"Super-user" privileges must only be used when actually needed

Users must not share their username or password (see action card ITS3) with anyone else, including IT support staff, or leave accounts logged in when they are away from a terminal

Third party users must be specifically authorised by the Information Asset Owner and the Head of Information Governance

**IT System restrictions:**

There is no direct write access to any PC and/or server

All software applications must be installed by IT

All access to another user's files must be authorised by a senior manager or director before access can be given by IT

High level system privileges will only be authorised where there is a specific requirement

**Guidance for Application Administrators:**

All application administrators must:

Control user access to information and system functions according to a defined system level access control policy

Prevent unauthorised access to any utility or system function that can override access controls

Protect the security of other systems with which information and resources are shared

Provide an audit function to enable the monitoring of successful and unsuccessful access to the system and the data contained therein.

**Login warnings:**

Warnings will be displayed on system login banners which shall say:

The system is for authorised users only

Usage is monitored

Evidence of misuse may result in legal proceedings

Supporting Document 1 - Equality Impact Assessment Tool

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

| | | Yes/No | Comments |
|---|---|---|---|
| **1.** | **Does the policy/guidance affect any one group less or more favourably than another on the basis of:** | | |
| | • Age | No | |
| | • Disability | No | |
| | • Gender reassignment | No | |
| | • Gender | No | |
| | • Race | No | |
| | • Religion or belief | No | |
| | • Sexual orientation including lesbian, gay and bisexual people | No | |
| | • Marriage and Civil Partnership | No | |
| | • Pregnancy and Maternity | No | |
| **2.** | **Is there any evidence that some groups are affected differently?** | No | |
| **3.** | **If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?** | NA | |
| **4.** | **Is the impact of the policy/guidance likely to be negative?** | NA | |
| **5.** | **If so can the impact be avoided?** | NA | |
| **6.** | **What alternatives are there to achieving the policy/guidance without the impact?** | NA | |
| **7.** | **Can we reduce the impact by taking different action?** | NA | |

Supporting Document 2 – Financial Impact Assessment Tool

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

| | Title of document: | Yes/No |
|---|---|---|
| **1.** | Does the implementation of this document require any additional Capital resources | |
| **2.** | Does the implementation of this document require additional revenue | |
| **3.** | Does the implementation of this document require additional manpower | |
| **4.** | Does the implementation of this document release any manpower costs through a change in practice | |
| **5.** | Are there additional staff training costs associated with implementing this document which cannot be delivered through current training programmes or allocated training times for staff | |
| | Other comments: | |

## Supporting Document 3 – Data Protection Impact Assessment

Please review the question below: Answering 'yes' to any of these questions is an indication that a DPIA is required

| | Title of document: | Yes/No |
|---|---|---|
| **1.** | Will the policy involve systematic and extensive profiling or automated decision-making to make significant decisions about people | Y/N |
| **2.** | Will the policy process special category data or criminal offence data on a large scale | Y/N |
| **3.** | Systematically monitor a publicly accessible place on a large scale | N |
| **4.** | Use new technologies | N |
| **5.** | Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit | N |
| **6.** | Carry out profiling on a large scale | N |
| **7.** | Process biometric or genetic data | N |
| **8.** | Combine, compare or match data from multiple sources | N |
| **9.** | Process personal data without providing a privacy notice directly to the individual | |
| **10.** | Process personal data in a way which involves tracking individuals online or offline location or behaviour | |
| **11** | Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them | |
| **12** | Process personal data which could result in a risk or physical harm in the event of a security breach | |
| **13** | Systematic processing of sensitive data or data of a highly personal nature | |
| **14** | Processing on a large scale | |
| **15** | Processing of data concerning vulnerable data subjects | |
| **16** | Innovative technological or organisational solutions | |

| | Title of document: | Yes/No |
|---|---|---|
| **17** | Processing involving preventing data subjects from exercising a right or using a service or contract | |
| **18** | Is this a major project involving the use of personal data | |
| | Comments:<br>**If we decide not to carry out a DPIA we document our reasons why**<br><br>**We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing** | |